

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA)	
)	
v.)	
)	19-cr-10063-DJC
RANDALL CRATER,)	
)	
Defendant)	

DEFENDANT RANDALL CRATER'S EXPERT SUMMARY

Defendant Randall Crater, by and through undersigned attorney, submits this summary of the expected expert testimony of Nodari Gogoberidze.

QUALIFICATIONS AND STATEMENT OF COMPENSATION

Nodari Gogoberidze is a Senior Software Engineer for the Broad Institute of Harvard and MIT. Mr. Gogoberidze has a Master of Liberal Arts (ALM) in Software Engineering from the Harvard Extension School. After graduating from Harvard, he taught a class on blockchain and Bitcoin where he taught the underpinnings of distributed systems, general blockchain principles, and the development of blockchain systems from first principles. During this course, Mr. Gogoberidze taught his students how to build a blockchain. A copy of his curriculum vitae is attached hereto as Exhibit "A."

Mr. Gogoberidze has been retained by Lawson & Weitzen, LLP as a testifying expert at the rate of \$225.00 per hour. His fee is not contingent on the outcome of the above-captioned criminal case. He has not previously testified as an expert.

INTRODUCTION

Attorney Lopez asked Mr. Gogoberidze to review the initial report and supplemental report prepared by Pamela Clegg of CipherTrace in this matter. Mr. Gogoberidze also evaluated the information that is available to the public about the My Big Coin cryptocurrency and, in particular, on GitHub. Mr. Gogoberidze also reviewed copies of My Big Coin accounts prior to June 2017 (DOJ0000396683-DOJ0000397875) as well as a print-out of transactions after June 2017 (DOJ0000082739-0000082924). As a result of this review, Mr. Gogoberidze has reached several conclusions about this case and Ms. Clegg's opinions. Mr. Gogoberidze's opinions are rendered to a reasonable degree of professional certainty.

CONCEPTUAL BACKGROUND

I. FUNDAMENTAL COMPONENTS OF A BLOCKCHAIN

The Blockchain was first described in *Bitcoin: A Peer-to-Peer Electronic Cash System* (Satoshi Nakamoto, 2008).¹ It was first implemented in the Bitcoin Blockchain. Since then, many new Blockchains have been developed, such as Ethereum and Algorand. In these differing Blockchain implementations, there are a large variety of differences in architecture, design, and technical complexity. Each Blockchain will have different considerations around permissions, privacy, security, data structures used, cryptographic schemes utilized, consensus algorithms, network model, and so on. There are however some common factors among all Blockchains.

¹ <https://nakamotoinstitute.org/>

At its most basic level, a Blockchain consists of data structures known as blocks, consisting of transactions between addresses, which are linked together in a linked list to form a chain of blocks.

A. Blocks

- A Block is the name given to a data structure
- The Block's body contains a set of transactions
- The Block's header contains a link or pointer to the previous block, by including the cryptographically secure hash of the previous block's header, forming the head of a chain of blocks
- The Block's header will contain other information, such as a timestamp of when it was created, and in the case of Proof of Work, a nonce (the solution to the cryptographic puzzle that miners must solve)

B. Transactions

- An address is derived from the public key of a cryptographically generated public-private key pair
 - usually prefixed with an identifier signifying address type
- The simplest transaction will contain a sender address, a recipient address, an amount of cryptocurrency to be sent, and fee to be paid to the node proposing the block (miner or verifier)
 - each transaction is cryptographically signed by the sender using their private key, verifiable by anyone using the sender's public key

C. Network

- A peer-to-peer network is formed by nodes
- Nodes have the responsibility of creating new blocks, verifying new blocks and their transactions, and storing the history of blocks
- In order to prevent malicious peers from misbehaving, blocks are proposed and accepted using a consensus algorithm
 - e.g., Proof of Work (PoW), Proof of Stake (PoS)
- Nodes are monetarily incentivized to provide these services
 - e.g., mining rewards, transaction fees
- Nodes engage with the network using software known as a Wallet
 - wallets may contain the user's credentials, such as public/private key pairs
 - wallets understand the underlying network protocols, and may refuse to engage with nodes not following the protocols

- wallets may engage with many networks, each with differing protocols
- A blockchain implementation may have more than one network
 - primary networks are usually called Mainnet
 - test networks, where there is no economic value for crypto coins, are usually called Testnets

D. Blockchain Implementations

There are many variations in implementing and building upon the fundamental components listed above. Bitcoin for example, has continued to be developed, and has grown in complexity since its original implementation. Transactions may now contain simple scripts. The Ethereum Blockchain is a full virtual machine, utilizing a concept known as a smart contract, where each transaction issues instructions for arbitrarily complex computations to be performed by the nodes of the network, so long as it is all paid for by the sender using the native cryptocurrency.

The original Bitcoin Blockchain discussed in Nakamoto's whitepaper, was envisioned as a fully decentralized, trustless, publicly accessible, peer-to-peer network, where the development was done via community consensus using fully open-source code. While this is still true of the main Bitcoin Blockchain, and many other Blockchains, it is not true of all Blockchains in general.

For instance, the Bitcoin source code is licensed under the MIT License.² While some open-source licenses such as GPL v3³ mandate that the source code, and all modifications to it, must be kept free and open source, the MIT License is fully

² <https://github.com/bitcoin/bitcoin/blob/master/COPYING>

³ <https://www.gnu.org/licenses/gpl-3.0.en.html>

permissive, allowing commercial and private use of the source code. This allows anyone to copy the Bitcoin source code, and make arbitrary modifications to it, including for instance making it a non-trustless system. While the wallets belonging to nodes on the main Bitcoin network may deny transactions from differing implementations, there is nothing preventing someone from creating their own network of nodes, with an entirely different set of network protocols, separate from the MainNet Bitcoin network. For example, someone can create a new network utilizing a unique consensus algorithm, or make it a completely private network only accessible by trusted peers.

Forking the Bitcoin Blockchain is not the only way to create new Blockchains and networks. The source code for Ethereum and Algorand for instance are not derivatives of Bitcoin, but instead are written entirely from scratch. While they share the common components of a Blockchain detailed above, they have many unique features not found in Bitcoin. They too are open-source and have been forked into derivative implementations. The Ethereum Foundation even developed and maintains a Private Enterprise version of Ethereum, entirely separate from the public MainNet implementation.⁴

E. Private Blockchains

A public Blockchain emphasizes decentralization, trustlessness, and open access. Fully public Blockchains are permissionless, and therefore may have

⁴ <https://ethereum.org/en/enterprise/private-ethereum/>

arbitrary network size, due to the very low barrier of entry. It is computationally easy to create an arbitrary number of new addresses. The number of nodes that are able to operate in the network is limited only by the amount of computing resources that an individual is willing to allocate. Because of this, public Blockchains are developed with the assumption of a hostile environment in the network, where malicious nodes exist and are trying to thwart or subvert the system. The network protocols and consensus algorithm used must assume that worst-case scenarios are not just possible but guaranteed. Transactions in most public Blockchains are not cryptographically encrypted, at least by default. This means all transactions, and the data they contain, are readable by anyone. There are however various mechanisms for private transactions in public Blockchains, including shielded transactions, and mechanisms for off-chain transactions.

Private Blockchains (sometimes erroneously equated with permissioned or consortium Blockchains) have controlled membership and access. They often operate in network environments under the assumption that the nodes in the network are non-adversarial. Due to their ability to lower security considerations, they tend to emphasize performance (high throughput of transactions), and the consensus algorithms used (e.g., Proof of Authority) tend not to be as computationally expensive as those found in public Blockchains, although there is no restriction from using Proof of Work or any other consensus algorithm. They also allow for confidentiality, in that Blockchain analysis cannot be conducted by individuals who do not have access privileges, and further transaction data may

be encrypted so that they are not viewable, without proper decryption privileges, even by members of the Blockchain.

Examples of private Blockchains include a version of Ethereum provided by the Enterprise Ethereum Alliance⁵, various projects under the Hyperledger Foundation (hosted by the Linux Foundation)⁶, and Quorum⁷ (originally developed by JP Morgan, and acquired by ConsenSys).

II. SUMMARY OF OPINIONS

In part 2, section 1 of Ms. Clegg's supplemental report dated May 18, 2022 (hereinafter "report"), the following definition of Blockchain Analysis is given: "Cryptocurrency blockchains are available to the public and reviewable on several platforms (e.g., Blockchain.com). Analysis of a blockchain can reveal, among other things, transactional history, trading frequency, block timing, and the total number of blocks."

The definition is correct, in that analysis of a Blockchain can reveal a number of details of the system and its contents, but there is no reason that a Blockchain must be fully amenable to Blockchain Analysis, while still meeting the criteria of being a Blockchain. Given the context laid out in the prior section, there are a number of ways to make transaction history and transaction details less transparent and therefore less amenable to analysis, even in public Blockchains. Private Blockchains,

⁵ <https://entethalliance.org/>

⁶ <https://www.hyperledger.org/>

⁷ <https://consensys.net/quorum/>

by definition, are only amenable to Blockchain Analysis if given the permission and proper access privileges.

Under Part 2, section 3 of the report, it is stated that “Based on blockchain analysis, MBC was not available as a cryptocurrency until June 28, 2017”. With respect to public Blockchains, there are a number of mechanisms that reduce the ability of Blockchain Analysis alone to decisively conclude that MBC could not have existed prior to June 28, 2017. For example, Bitcoin has a scripting language allowing transaction issuers to embed small amounts of arbitrary metadata onto the Bitcoin Blockchain. This mechanism has been used to derive so-called “Colored Coins”⁸, alternative cryptocurrencies that live within Bitcoin alongside its native cryptocurrency, BTC. Unlike transactions of BTC, which have dedicated fields in the transaction data format, Colored Coin transactions are embedded as metadata, in an arbitrary format dictated by the currency creator, and may even be in encrypted form, if so designed. Therefore, Colored Coin transactions are less susceptible to analysis of the sort that BTC is susceptible to. It is also possible that MBC existed as a private cryptocurrency, on a private Blockchain, prior to June 28, 2017, in which case no amount of Blockchain Analysis using public databases, exchanges, indexes or trackers would conclusively prove its existence or non-existence.

In part 2, section 1 of the report, the following definition is given of a fork: “A fork occurs when there is a change to the blockchain protocol of a cryptocurrency. A fork is always based on the original blockchain such that all transactions from the

⁸ https://en.bitcoin.it/wiki/Colored_Coins

original blockchain are copied onto the subsequent blockchain(s).” In part 3, section 3 of the report, it is stated that “There is no evidence of a ‘fork’ on the MBC blockchain prior to [June 28, 2017].”

It is predominantly the case that all transactions from the original Blockchain are copied onto the subsequent Blockchain, in both soft and hard forks, but it is not always the case. A widely cited example where transaction history was overwritten due to a fork is described in Ethereum Improvement Proposal (EIP) 779⁹, and is known as the DAO Fork. As described in EIP-779, “the DAO Fork was an ‘irregular state change’ that transferred ether balances from a list of accounts (‘child DAO’ contracts) into a specified account (the ‘WithdrawDAO’ contract).” In general, there is no stipulation which mandates that a hard fork must maintain a full history of transactions prior to the fork.

Also, there is precedent that prior to the launch of a public Blockchain, and its corresponding Genesis block being instantiated, some amount of initial funds are accumulated during a presale. The most famous example is the presale leading up to Ethereum version 1¹⁰, after which Ether, the cryptocurrency native to Ethereum, was distributed to the 8,993¹¹ accounts that had previously funded the project. In the case of Ethereum, all 8,993 distributions were included in the Genesis block, however there is no requirement that this be the case for all Blockchains. It is certainly

⁹ <https://eips.ethereum.org/EIPS/eip-779>

¹⁰ <https://blog.ethereum.org/2015/07/30/ethereum-launches/>

¹¹ <https://etherscan.io/txs?block=0>

possible to distribute cryptocurrency, proportional to funds received during a presale, to the respective accounts, over multiple blocks.

The foregoing opinions are rendered to a reasonable degree of professional certainty based on the information that was made available to Nodari Gogoberidze as of the date of this summary. Mr. Gogoberidze reserves the right to supplement and/or amend this summary, and his opinions, in the event that additional information becomes available.

Respectfully submitted,
For the Defendant,
Randall Crater
By his attorneys:

/s/ Scott P. Lopez
Scott P. Lopez, BBO # 549556
splopez@lawson-weitzen.com
LAWSON & WEITZEN, LLP
88 Black Falcon Ave, Suite 345
Boston, MA 02210
617-439-4990 (tel.)
617-439-3987 (fax)

Dated: June 21, 2022

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) on June 21, 2022.

/s/ Scott P. Lopez
Scott P. Lopez